Treasury bureaus and the Departmental Offices may establish more stringent standards for their own use. Whenever new security equipment is procured, it shall be in conformance with the standards and specifications referred to above and shall, to the maximum extent practicable, be of the type available through the Federal Supply System.

§ 2.26 Accountability procedures [4.1(b)].

(a) *Top Secret Control Officers.* Each Treasury bureau and the Departmental Offices shall designate a primary and alternate Top Secret Control Officer. Within the Departmental Offices, the Top Secret Control Officer function will be established in the Office of the Executive Secretary for collateral Top Secret information and in the Office of the Special Assistant to the Secretary (National Security) with respect to sensitive compartmented information. The term ''collateral'' refers to national security information classified Confidential, Secret, or Top Secret under the provisions of Executive Order 12356 or prior Orders, for which special intelligence community systems of compartmentation (such as sensitive compartmented information) or special access programs are not formally established. Top Secret Control Officers so designated must have a Top Secret security clearance and shall:

(1) Initially receive all Top Secret information entering their respective bureau, including the Departmental Offices. Any Top Secret information received by a Treasury bureau or Departmental Offices employee shall be immediately hand carried to the designated Top Secret Control Officer for proper accountability.

(2) Maintain current accountability records of Top Secret information received within their bureau or office.

(3) Ensure that Top Secret information is properly stored and that Top Secret information under their control is personally destroyed, when required. Top Secret information must be destroyed in the presence of an appropriately cleared official who shall actually witness such destruction. Accordingly, the use of burnbags to store Top Secret information, pending final destruction at a later date, is not authorized.

(4) Ensure that prohibitions against reproduction of Top Secret information are strictly followed.

(5) Conduct annual physical inventories of Top Secret information. An inventory shall be conducted in the presence of an individual with an appropriate security clearance. The inventory shall be completed annually and signed by the Top Secret Control Officer and the witnessing individual.

(6) Ensure that Top Secret documents are downgraded, declassified, retired or destroyed as required by regulations or other markings.

(7) Attach a TD F 71–01.7 (Top Secret Document Record) to the first page or cover of each copy of Top Secret information. The Top Secret Document Record shall be completed by the Top Secret Control Officer and shall serve as a permanent record.

(8) Ensure that all persons having access to Top Secret information sign the Top Secret Document Record. This also includes persons to whom oral disclosure of the contents is made.

(9) Maintain receipts concerning the transfer and destruction of Top Secret information. Record all such actions on the Top Secret Document Record which shall be retained for a minimum of three years.

(10) As received, number in sequence each Top Secret document in a calendar year series (e.g. TS 89–001). This number shall be posted on the face of the document and on all forms required for control of Top Secret information.

(11) Attach a properly executed TD F 71–01.5 (Classified Document Record of Transmittal) when a Top Secret document is transmitted internally or externally.

(12) Verify, prior to releasing Top Secret information, that the recipient has both a security clearance and is authorized access to such information.

(13) Report, in writing, all Top Secret documents unaccounted for to the Assistant Secretary (Management) who shall take appropriate action in conjunction with the Departmental Director of Security.

(14) Assure that no individual within his or her office or bureau transmits

Top Secret information to another individual or office without the knowledge and consent of the Top Secret Control Officer.

(15) Ensure upon receipt that a Standard Form 703 (Top Secret Cover Sheet) is affixed to such information.

(16) Notify office and/or bureau employees annually in writing of the designated control point for all incoming and outgoing Top Secret information.

(17) Be notified as to the transmission, per §2.28(b), whenever Top Secret information is sent outside of a Treasury bureau or office within the Departmental Offices.

(b) *Top Secret Control Officer Listings.* In order for the Departmental Director of Security to maintain a current listing of Top Secret Control Officers within the Department, each Treasury bureau and the Departmental Offices shall annually report each October 15th in writing to the Departmental Office of Security, the identities of the office(s) and names of the officials designated as their primary and alternate Top Secret Control Officers. Any changes in these designations shall be reported to the Departmental Director of Security within thirty days.

(c) *Top Secret Document Record.* Upon receipt in the Department a green, color coded, TD F 71–01.7 (Top Secret Document Record) shall be attached by the Top Secret Control Officer to the first page or cover of the original and each copy of Top Secret information. The Top Secret Document Record shall remain attached to the Top Secret information until it is either transferred to another United States Government agency, downgraded, declassified or destroyed. The Top Secret Document Record, which shall initially be completed by the Top Secret Control Officer, shall identify the Top Secret information attached, and shall serve as a permanent record of the information. All persons, including stenographic and clerical personnel, having access to the information attached to the Top Secret Document Record must list their name and the date on the TD F 71–01.7 prior to accepting responsibility for its custody. The TD F 71–01.7 shall also indicate those individuals to whom only oral disclosure of the contents is made. Whenever any Top Secret information is transferred to another United States Government agency, downgraded, declassified or destroyed, the Top Secret Control Officer shall record the action on the Top Secret Document Record and retain it for a minimum or three years after which time it may be destroyed. In order to maintain the integrity of the color coding process the photocopying and use of non-color coded Top Secret Document Record forms is prohibited.

(d) *Classified Document Record of Transmittal.* TD F 71–01.5 (Classified Document Record of Transmittal) shall be the exclusive classified document accountability record for use within the Department of the Treasury. No other logs or records shall be required except for the use of TD F 71–01.7 which is applicable to Top Secret information. TD F 71–01.5 shall be used for single or multiple document receipting and for internal and external routing. The inclusion of classified information on TD F 71–01.5 is to be avoided. In the event the subject title is classified, a recognizable short title shall be used, e.g., first letter of each word in the subject title. Several items may be transmitted to the same addressee with one TD F 71–01.5. TD F's 71–01.5 shall be maintained for a three year period after which the form may be destroyed. No record of the actual destruction of the TD F 71–01.5 is necessary.

(1) *Top Secret Information.* Top Secret information shall be subject to a continuous receipt system regardless of how brief the period of custody. TD F 71–01.5 shall be used for this purpose. Top Secret accountability records shall be maintained by Top Secret Control Officers separately from the accountability records of other classified information.

(2) *Secret Information.* Receipt on TD F 71–01.5 shall be required for transmission of Secret information between bureaus, offices and separate agencies. Responsible office heads shall determine administrative procedures required for the internal control within their respective offices. The volume of classified information handled and personnel resources available must be considered in determining the level of adequate security measures while at the

same time maintaining operational efficiency.

(3) *Confidential and Limited Official Use Information*. Receipts for Confidential and Limited Official Use information shall not be required unless the originator indicates that receipting is necessary.

[55 FR 1644, Jan. 17, 1990; 55 FR 13134, Apr. 9, 1990]

§ 2.27 Storage [4.1(b)].

Classified information shall be stored only in facilities or under conditions designed to prevent unauthorized persons from gaining access to it.

(a) *Minimum Requirements for Physical Barriers*—(1) *Top Secret*. Top Secret information shall be stored in a GSA-approved security container with an approved, built-in, three-position, dial-type, changeable, combination lock; in a vault protected by an alarm system and response force; or in other types of storage facilities that meet the standards for Top Secret information established under the provisions of § 2.25. Top Secret information stored outside the United States must be in a facility afforded diplomatic status. One or more of the following supplementary controls is required:

(i) The area that houses the security container or vault shall be subject to the continuous protection of U.S. guard or duty personnel;

(ii) U.S. Guard or duty personnel shall inspect the security container or vault at least once every two hours; or

(iii) The security container or vault shall be controlled by an alarm system to which a force will respond in person within 15 minutes.

Within the United States, the designated security officer in each Treasury bureau and the Department Offices shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored. Any vault used for the storage of sensitive compartmented information shall be configured to the specifications of the Director of Central Intelligence. Prior to an office or bureau operating such a vault, formal written certification for its use must first be obtained from the Special Assistant to the Secretary (National Security) as the senior Treasury official of the Intelligence Community.

(2) *Secret and Confidential*. Secret and Confidential information shall be stored in a manner and under the conditions prescribed for Top Secret information, or in a container, vault, or alarmed area that meets the standards for Secret or Confidential information established under the provisions of § 2.25. Secret and Confidential information may also be stored in a safe-type filing cabinet having a built-in, three-position, dial-type, changeable, combination lock, and may continue to be stored in a steel filing cabinet equipped with a steel lock-bar secured by a GSA-approved three-position, dial-type, changeable, combination padlock. The modification, however, of steel filing cabinets to barlock-type as storage equipment for classified information and material is prohibited and efforts are to be made to selectively phase out the use of such barlock cabinets for storage of Secret information. Exceptions may be authorized only by the Departmental Director of Security upon written request from the designated bureau security officer. The designated security officer in each Treasury bureau and the Departmental Offices shall prescribe those supplementary controls deemed necessary to restrict unauthorized access to areas in which such information is stored. Access to bulky Secret and Confidential material in weapons storage areas, strong rooms, evidence vaults, closed areas or similar facilities shall be controlled in accordance with requirements approved by the Department. At a minimum, such requirements shall prescribe the use of GSA-approved, key-operated, high-security padlocks. For Secret and Confidential information stored outside the United States, it shall be stored in the manner authorized for Top Secret, in a GSA-approved safe file, or in a barlick cabinet equipped with a security-approved combination padlock if the cabinet is located in a security-approved vault and/or in a restricted area to which access is controlled by United States citizen personnel on a 24-hour basis.

(b) *Combinations*—(1) *Equipment in Service*. Combinations to dial-type, changeable, combination locks shall be